



# Mist Integration with ISE for Guest Access





# **Table of Contents**

FLOW OF GUEST ACCESS VIA RADIUS SERVER USING MAB		
MIST AP CONFIGURATION	4	
WLAN CONFIGURATION	4	
AUTHENTICATION POLICY	5	
AUTHORIZATION PROFILE	6	
URL REDIRECT	7	
COA(CHANGE OF AUTHORIZATION)	8	
SECOND ACCESS REQUEST AND PERMIT ACCESS	8	



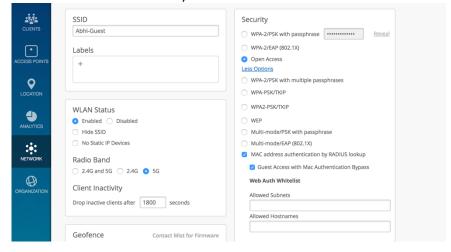
# Flow of Guest Access via Radius Server using MAB

- 1) Wireless MAB WLAN is created on the Mist AP with MAB being performed via Radius Lookup.
- 2) When a client associated to this WLAN, the the mac address of the client is sent across to the radius server via an ACCESS REQUEST
- 3) Radius server looks up its database and if the client is not found in the database, sends back a ACCESS ACCEPT with a redirection URL to the Mist AP
- 4) The client now is provided with limited access to the network which includes access to the BOOTP, DNS and Radius server
- 5) After the client receives an IP, the AP opens a web socket to and listens to any HTTP traffic initiated from the client
- 6) Any HTTP traffic initiated from the client is intercepted and is responded with a URL that was sent by Radius server
- 7) The client is presented with URL. Based on the policy: it might be a sponsored portal, a self registration portal or a hotspot portal.
- 8) Once the client provides necessary info on the URL, the ISE now install this client's mac address in its database and also issues a CoA (Change of Authorization) request with a command to re-authorize this client.
- 9) The Mist AP upon receiving the CoA request acknowledges the request and sends back the same ACCESS REQUEST as in step 2.
- 10) At this point the client is available in the radius server database and hence would be provided with a ACCESS-ACCEPT without any restrictions of URL-Redirect and the client would have network connectivity based on the policies defined.

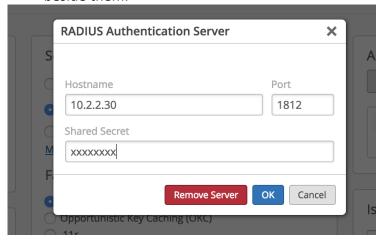


# **WLAN Configuration**

- a. Network -> WLAN -> Add WLANs
- b. Enable "MAB by Radius lookup" and "Guest Access with MAB" under it
- c. You can use the Whitelist in order to permit specific subnets/hostnames when the client is in the redirect state (It is optional if left blank, the radius server is the only IP that is whitelisted for access)



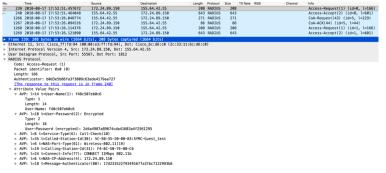
- d. Add the Radius Server of Choice (RadSec is disabled when not used)
  - i. Click on the Radius server and it will provide an option to input the Radius Server details (IP, Port, Shared Secret) which would be the Radius server IP and port details
- ii. You would also have the option of adding a secondary-server/tertiary servers
- iii. You will also be edit the order of the preference for servers using the arrow keys place beside them.



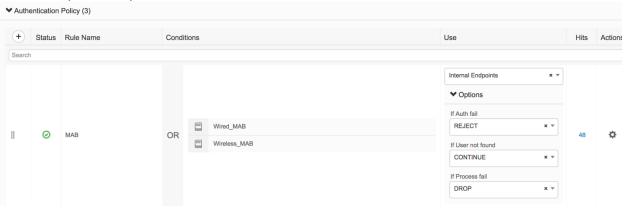


### **Authentication Policy**

a. When a client associates to this WLAN, the access point sends a ACCESS-REQUEST to Radius Server



b. The packet capture above indicates the ACCESS-REQUEST sent across from the client



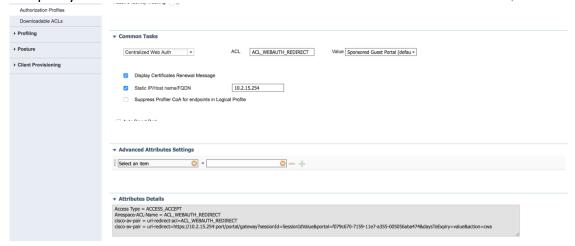
c. The authentication policy on the radius server is tailored to "continue" if the user is not found in the database. This allows the client to get an IP and be placed in the redirect state.



- d. The authorization policy has two policies that will be hit during the process of this guest access flow. The first policy that is hit as indicated above is
  - "Wifi\_Redirect\_to\_Guest\_Login" which provides partial access to the client.
    - Note: Upon successful auth after CoA we hit the second auth indicated as "Wifi\_Guest\_Access" which provides full access to the client

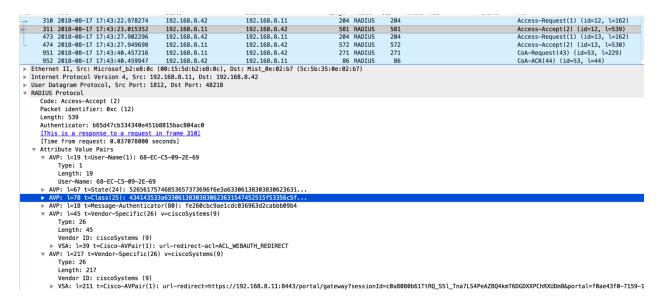


Once we hit the first policy MAB policy on the Radius server, the server responds with an Access-Accept to the Mist AP but also provides a redirect URL which is presented to the client. The policy is created as below in the radius server



The Radius server response would contain the above URL as shown in the packet capture below.

Note: Although there is an ACL that is presented as well as a part of the response, at Mist, we wouldn't need to configure any ACL/WxLAN policies as the we have a built in wall garden policy which provide BOOTP, DNS and ISE server access only to the client.





#### **URL** redirect

- At this stage, client is able to procure an IP.
- The client should initiate an HTTP transaction by logging into the browser and trying to reach an external URL
- Any HTTP traffic initiated from the client is intercepted and is responded with a URL that was sent by Radius server
- The client is presented with URL. Based on the policy: it might be a sponsored portal, a self registration portal or a hotspot portal.
- Once the client provides necessary info on the URL, the radius server now installs this client's mac address in its database and also issues a CoA (Change of Authorization) request with a command to re-authorize this client.

No.		Time		Source	Destination		Protocol		Kate RSSI	Channel	Into
			7 17:43:27.949698	192.168.8.11	192.168.8.42		RADIUS	572			Access-Accept(2) (id=13, l=530)
→			7 17:43:40.457216	192.168.8.11	192.168.8.42		RADIUS	271			CoA-Request(43) (id=53, l=229)
4			7 17:43:40.459947	192.168.8.42	192.168.8.11		RADIUS	86			CoA-ACK(44) (id=53, l=44)
			7 17:43:40.462132	192.168.8.42	192.168.8.11		RADIUS	204			Access-Request(1) (id=13, l=162)
			7 17:43:41.069095	192.168.8.11	192.168.8.42		RADIUS	286			Access-Accept(2) (id=13, l=244)
			7 17:44:13.398105	192.168.8.11	192.168.8.42	271	RADIUS	271			CoA-Request(43) (id=54, l=229)
			tes on wire (2168 b:								
▶	▶ Ethernet II, Src: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c), Dst: Mist_0e:02:b7 (5c:5b:35:0e:02:b7)										
-	▶ Internet Protocol Version 4, Src: 192.168.8.11, Dst: 192.168.8.42										
▶	User D	atagram Pro	tocol, Src Port: 413	351, Dst Port: 3799							
₩	RADIUS	Protocol									
	Cod	e: CoA-Reque	est (43)								
	Pac	ket identifi	ier: 0x35 (53)								
	Len	gth: 229									
	Aut	henticator:	190cded5bd49afdff47	bcb87c7245d90							
	[Th	e response t	to this request is i	n frame 952]							
	<b>▼ Att</b>	ribute Value	e Pairs								
	▶ A	NVP: l=6 t=N	AS-IP-Address(4): 19	92.168.8.42							
▶ AVP: l=19 t=Calling-Station-Id(31): 68-EC-C5-09-2E-69											
► AVP: 1=6 t=Event=Timestamp(55): Aug 17, 2018 17:43:40.00000000 PDT											
	▶ A	VP: l=18 t=	Message-Authenticate	or(80): 58413c1fb15	355502a0551858f0160f4						
			Vendor-Specific(26)								
		Type: 26									
		Length: 43	3								
			: ciscoSystems (9)								
	1		t=Cisco-AVPair(1):	subscriber: reauther	ticate-type=last						
	<pre>v AVP: l=41 t=Vendor-Specific(26) v=ciscoSystems(9) Type: 26</pre>										
Type: 20 Lenath: 41											
Vendor ID: ciscoSystems (9)											
▶ VSA: 1=35 t=Cisco-AVPair(1): subscriber:command=reauthenticate											
	<pre># VSA: 1=35 t=Lisco-Avrair(1): Subscriber: Commandereauthenticate # AVP: l=76 t=Vendor-Specific(26) v=ciscoSystems(9)     Type: 26</pre>										
Length: 76  Vendor ID: ciscoSystems (9)											
► VSA: 1=70 t=Cisco-AVPair(1): audit-session-id=c0a8080b61TtRO SS\ Tna7LS4PeAZB04kmTGDGDXXPChRXUDm8											
		- V3M. (=/0	C-CISCO-AVPAIR(I):	auatr-session-in-tr-ce	a000000011 chQ_33 (_111a/L34F	CALDQ4KIII I OL	ODAKPCIII	MUDIIIO			

#### Note:

- 1) The key observation in the CoA request is that Cisco AV pair Subscriber:Command has the value "reauthenticate". This is the reason why we are able to authorize a client for the second time around without having to disconnect the client.
- 2) The Cisco AV pair Subscriber:Reauthenticate-type has the value "last" which indicates that the Mist AP should use the same access request as it presented the last time for the client in question.



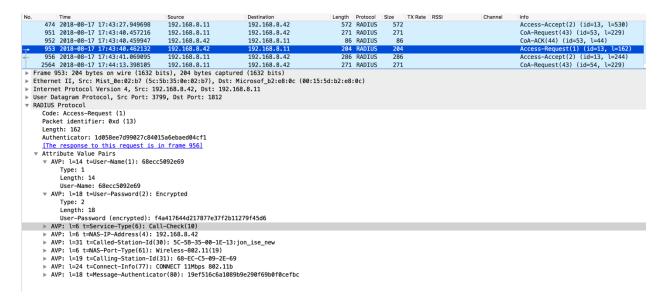
## CoA(Change of Authorization)

### We acknowledge this CoA request using a CoA Ack

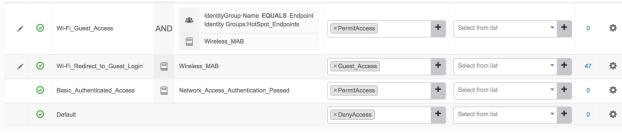
т	951 2018-08-17 17:43:40.457216	192.168.8.11	192.168.8.42	271 RADIUS	271	CoA-Request(43) (id=53, l=229)		
4	952 2018-08-17 17:43:40.459947	192.168.8.42	192.168.8.11	86 RADIUS	86	CoA-ACK(44) (id=53, l=44)		
	953 2018-08-17 17:43:40.462132	192.168.8.42	192.168.8.11	204 RADIUS	204	Access-Request(1) (id=13, l=162)		
	956 2018-08-17 17:43:41.069095	192.168.8.11	192.168.8.42	286 RADIUS	286	Access-Accept(2) (id=13, l=244)		
İ	2564 2018-08-17 17:44:13.398105	192.168.8.11	192.168.8.42	271 RADIUS	271	CoA-Request(43) (id=54, l=229)		
	Frame 952: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)							
-	▶ Ethernet II, Src: Mist_0e:02:b7 (5c:5b:35:0e:02:b7), Dst: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c)							
-	▶ Internet Protocol Version 4, Src: 192.168.8.42, Dst: 192.168.8.11							
-	▶ User Datagram Protocol, Src Port: 3799, Dst Port: 41351							
7	▼ RADIUS Protocol							
	Code: CoA-ACK (44)							
Packet identifier: 0x35 (53)								
	Length: 44							
	Authenticator: de7370fd09f7d5dddceb232f33b2e51f							
	[This is a response to a request in frame 951]							
	[Time from request: 0.002731000 seconds]							
	▼ Attribute Value Pairs							
	▶ AVP: l=6 t=Event-Timestamp(55): Aug 17, 2018 17:43:40.000000000 PDT							
	▶ AVP: l=18 t=Message-Authenticator(80): 9013d7fde7f0d353e6c1b5de6040b0e9							

## **Second Access Request and Permit Access**

- Based on the CoA request – we send the same ACCESS REQUEST back to the client



- At this point - the client is available in the radius server database and hence we hit the second policy from the authorization policy perspective.



In the above example – we would meet the criteria for the policy named "Wifi\_Guest\_Access" since the hotspot clients are stored in the Hotspot\_Endpoints Identity Group. Hence the client would be provided



with a ACCESS-ACCEPT without any restrictions of URL-Redirect and the client would have network connectivity based on the policies defined which in this case is "PermitAccess"